PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#10
DBuller
6-21-02

In re Application of:
David J. Kinsella

Serial No.: 09/584,162

Filed: May 30, 2000

For: POINTING DEVICE WITH BIOMETRIC SENSOR

Group Art Unit: 2623

Examiner: Bali, Vikkram.

Atty. Dkt. No.: KINS:002USC2/10026193

CERTIFICATE OF MAILING
37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on the date below:

June 11, 2002 (Date) — Michael C. Barrett (Michael C. Barrett)

APPEAL BRIEF

BOX AF
Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Applicant hereby submits an original and two copies of this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated January 2, 2002. The Notice of Appeal was filed on April 2, 2002, and the Mail Room date of receipt of the Notice of Appeal was April 11, 2002. Pursuant to 37 C.F.R. § 1.17(c), a check in the amount of $160.00 is enclosed to cover the fee for filing a brief in support of an appeal. No extension fees are believed to be required.

06/20/2002 ANJOHN1 00000056 09584162
01 FC:220 160.00 OP

Should payment for the fee be deficient or absent, or if any additional fees are required for any reason, please withdraw the appropriate amount from Fulbright & Jaworski Deposit Account No.: 50-1212/10026193/MCB.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is the inventor, David J. Kinsella.

II. RELATED APPEALS AND INTERFERENCES

At present, there are no related appeals or interferences.

III. STATUS OF THE CLAIMS

The present application is a continuation application of Serial No. 08/940,553.

Claims 1-48 of the present application were filed concurrently with a Preliminary Amendment canceling claims 3-6 and 25-48, adding claims 49-81, and amending claims 1, 2, 7-9, and 18. In response to a first Office Action, Applicant amended independent claims 1, 61, 67, 71 and 79 and canceled claims 62-66. Filed concurrently herewith is an Amendment (a copy of which is attached as Exhibit B), conforming to 37 C.F.R. § 1.116, that cancels without prejudice claim 59 and makes amendments of form to claims 1 and 61.

Claims 1, 2, 7-24, 49-58, 60-61 and 67-81 remain pending and are being appealed. Those claims are listed in Exhibit A.

IV. STATUS OF AMENDMENTS

The Amendment of Exhibit B corrects a spelling error discovered in claims 1 and 61 and deletes an extraneous occurrence of the word "and" from claim 61. The spelling correction changes "depressable" to "depressible." Additionally, claim 59 has been canceled. The amendments conform with 37 C.F.R. § 1.116 [*See also* MPEP § 1207], and Applicant correspondingly requests their entry and consideration during this appeal. As of the time of filing of this Brief, the amendments had not been considered or acted upon by any Examiner.

V. SUMMARY OF THE INVENTION

The inventions embodied by the appealed claims involve pointing devices (such as computer mice or trackballs), verification systems, and methods for verifying a user of an electronic system coupled to a biometric sensor (such as a fingerprint sensor). [*See* preambles of independent claims 1, 61, 67, 71, and 79]. These inventions increase security of computerized systems. [Specification, page 16 (providing an example of the invention preventing fraud)]. Importantly, each of the appealed claims contains a verification system including a "user storage," an "authorization profile storage," and an "audit log storage." These features, and particularly the authorization profile storage and audit log storage, arguably form the heart of this appeal.

In a representative embodiment, a computer mouse is equipped with a fingerprint sensor, which continuously verifies the identity of a user by comparing the user's fingerprint with fingerprints of authorized users stored in a "user storage." [Specification, pages 14-15 (describing the user storage)]. Additionally, the mouse keeps track of allowable transaction parameters stored in an "authorization profile storage" for that user. [Specification, pages 14-15 (describing the authorization profile)]. The authorization profile storage dictates permissible dates, times, functions, transactions, or machines that an authorized user can use. [Id.]. For example, an authorization profile storage may indicate that authorized user A is allowed to use a computer mouse to engage in specific transaction X only at time-of-day Y. [*See* Id.].

If a user is not verified or if she attempts a transaction not allowed by the authorization profile storage, the transaction is blocked and the user's fingerprint (or other information concerning one's identity) may be stored in an "audit log storage" along with a description of the transaction that was being attempted. [Specification, pages 15-16 (describing the audit log

storage)]. In one embodiment, the audit log storage keeps track of not only failed or unauthorized transaction attempts, but also successful transactions as well. [Id.]

With the user storage, authorization profile storage, and audit log storage in place, computer security is increased, and those attempting to breach security may be readily identified. [Specification, page 16 (providing an example situation in which the security of a cash register system is increased)]. Further, the nature of attempted security breaches may be ascertained by referring to the audit log storage. [*See* Id.].

The specification succinctly explains these important security concepts, with reference to Figure 9, as follows:

> [W]hen a user attempts to access the system, his or her fingerprint is read by device 203, and compared with the known user storage 226 and the authorization profile storage 222 to determine whether to allow the particular user to perform the function requested. ... The identification of the user is verified continuously as long as the user is in contact with the biometric input device 203 (for this example, the computer trackball pointing device 10). Each time the user inputs a system request, the verification process must be completed and maintained prior to continuing the use of the device being accessed.
>
> * * *
>
> If, at any time, a biometric reading is taken which does not match any user having a profile stored in the known user storage 226, access is denied and an audit log may be stored within the audit log storage 224 to provide a record of unsuccessful access attempts. Such an audit log entry may include time, date, attempted transaction, and a copy of the user identification information determined by the biometric device, such as a scanned fingerprint image, a fingerprint minutia representation, or others. Alternatively, if the user identifying information from the biometric device is matched with a user found in the known user storage 226, but the authorization profile storage 222 indicates that the particular user has requested something for which he or she is not authorized, then access is also denied and an audit log entry is also created in the audit log storage 224. This entry may include time, date, attempted transaction, and an indication of the user's identity, such as a name, a photographic image, or others.
>
> Such an audit log affords a significant capability to detect internal fraud and other unauthorized use by persons known to the system, and indeed authorized to perform some tasks, but not authorized for the task or function at the attempted time or date.

[Specification, pages 15-16 (emphasis added)].

Claim 1 is directed to a pointing device, such as a computer mouse or trackball. [*See* claim 1]. The pointing device includes an interface for communicating with an electronic system, a position sensor, a button for conveying information, a biometric sensor, and the verification system outlined above. [Id.]. The interface simply allows the pointing device to communicate with an electronic system, and is shown in Figure 1 as a cable running from a trackball. [Specification, pages 7-8, Figure 1 (element #20)]. The position sensor conveys positional information as the pointing device moves about. [*See, e.g.*, Specification, page 5]. The button of the pointing device allows a user to make a selection by clicking the button. [Id.; *also* Figure 1 (element #22a)]. The biometric sensor reads biometric information from the user, and in a representative embodiment, is a fingerprint sensor located at or near a button of the pointing device. [Specification, page 8 (stating that a fingerprint sensor may be mounted below the center button of a trackball)].

The verification system recited in claim 1 is the security system described above, which includes the user storage, the authorization profile storage, and the audit log storage. [Specification, pages 14-16]. The user storage stores identification information of authorized users, which is compared with information read by the biometric sensor to verify the identity of a user. [Specification, page 14]. The authorization profile storage stores permissible dates, times, functions, transactions, or machines associated with a particular authorized user. [Id.]. Finally, the audit log storage keeps track of unsuccessful transactions and transaction attempts. [Specification, pages 14-16]. In particular, the audit log storage is configured to store (a) user identification information when access is denied to a system [Specification, page 15] and (b) user

identification information and attempted transaction information when a specific transaction is denied within the system. [Specification, pages 15-16].

Independent claim 61 is similar to claim 1 except that the biometric sensor of claim 61 reads information from a *toe* of a user instead of from a finger. Independent claim 67 focuses exclusively on the computer verification system summarized above and accordingly includes a processor and a memory that includes the user storage, authorization profile storage, and audit log storage. Independent claim 71 is directed to a method for verifying a user and includes steps embodying the functionality of the user storage, authorization profile storage, and audit log storage. Independent claim 79 is also directed to the verification system and recites that the audit log storage stores information in response to (a) successful transactions, (b) denial of access to the electronic system, and (c) denial of access to perform a specific action within the electronic system.

Dependent claims define further characteristics of the pointing devices and verification systems/methods. For example, claims 56-58 define a combined identification/substance detection embodiment, which allows substance detection to occur along with biometric detection. [*See* specification, page 17]. This allows, for example, a user to be denied access to a system if (a) his fingerprint doesn't match a user storage fingerprint, (b) his attempted transaction is not allowed by the authorization profile storage, or (c) e.g., his blood alcohol content is too high. [*See* Specification, page 17].

VI. ISSUES ON APPEAL

The issues to be resolved on appeal are:

1. Are claims 1, 2, 10, 11-14, 49-56 and 60 rendered obvious by U.S. Patent No. 5,229,764 ("Matchett") in view of U.S. Patent No. 5,513,272 ("Bogosian")?
2. Are claims 7-9, 20 and 21 rendered obvious by Matchett in view of Bogosian and further in view of Applicant's "admitted prior art"?
3. Are claims 15-19 rendered obvious by Matchett in view of Bogosian and further in view of U.S. Patent No. 5,703,356 ("Bidiville")?
4. Are claims 22-24 rendered obvious by Matchett in view of Bogosian and further in view of U.S. Patent No. 5,838,306 ("O'Connor")?
5. Are claims 61 and 67-81 rendered obvious because they claim similar subject matter as claims 1-24 and 49-60?
6. Are claims 57 and 58 rendered obvious by Matchett in view of Bogosian and further in view of U.S. Patent NO. 5,337,358 ("Axelrod")?

All of these issues may be boiled-down to the following single issue: does the cited art, taken alone or in any combination, teach or suggest the combination of the authorization profile storage and audit log storage recited in each and every claim?

VII. GROUPING OF THE CLAIMS

Independent claims 1, 61, 67, 71, and 79 are each asserted to be independently patentable, for similar reasons. The dependent claims stand or fall with their independent claims.

VIII. ARGUMENT

A. Summary of Argument

All the pending claims are allowable because none of the cited art, taken alone or in any combination, discloses or suggests the claimed authorization profile storage or audit log storage. Moreover, none of the cited art discloses or suggests the claimed combination of those two features nor provides any motivation to come to that combination.

B. Taken alone or in any combination, Matchett in view of Bogosian (or further in view of Automatic Teller Machines) does not render claims 1, 2, 10, 11-14, 49-56, or 60 unpatentable

Claims 1, 2, 10, 11-14, 49-56 and 60 stand rejected as being obvious under 35 U.S.C. § 103 in view of Matchett combined with Bogosian. Applicant respectfully traverses and directs his arguments to independent claim 1. Dependent claims 2, 10, 11-14, 49-56, and 60 stand or fall with claim 1.

1. Neither Matchett nor Bogosian discloses or suggests the claimed authorization profile storage

Independent claim 1 recites a verification system including the authorization profile. As explained in the specification (*e.g.*, pages 14-15), the authorization profile may be used in certain embodiments to define, for example, permissible dates, times, and functions that a specific person can perform within a specific electronic system. Such a feature is *nowhere* disclosed or even suggested by Matchett or Bogosian (taken alone or in combination). In fact, the Examiner never even contends that Matchett or Bogosian contains the recited authorization profile. Correspondingly, Applicant respectfully contends that the cited art is clearly insufficient to support this rejection.

2. Neither Matchett nor Bogosian discloses or suggests the claimed audit log storage

Independent claim 1 recites that the audit log storage stores the following:

> (a) user identification information from said biometric sensor in response to a denial of access to said electronic system; and
>
> (b) user identification information from said biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within said electronic system.

Such features are nowhere disclosed or even suggested by Matchett or Bogosian (taken alone or in combination).

In contrast, Bogosian is directed to a system for verifying the use of a credit or identification card, in which "access" to the card is totally granted (allowing the user to use the card without restriction) or totally denied (confiscating the card from the user). [Bogosian, Abstract.] In particular, the disclosure of Bogosian involves several sequential verification steps:

> (1) scan information from the magnetic tape of the card and compare it to corresponding information in a database — if there is not a match, confiscate the card prior to use;
>
> (2) scan the surface of the card (to check for tampering) and compare it to corresponding information in a database — if there is not a match, confiscate the card prior to use;
>
> (3) take a fingerprint of the *user* of the card and compare it to the *owner's* fingerprint information printed on the card and the owner's fingerprint information in a database — if there is no match, confiscate the card prior to use and record the fingerprint of the user;
>
> (4) perform additional verification measures (such as voice, retina), if necessary.

[Bogosian, FIG. 1; col. 2, lines 17-63; col. 5, lines 24-34].

Bogosian does not disclose or even suggest storing user identification information (*e.g.*, a fingerprint) and attempted transaction information in response to a denial of access to perform a specific transaction within an electronic system, as recited in claim 1. The only time Bogosian stores a user's fingerprint is when the card is confiscated (and, hence, the card cannot even be used to attempt a transaction). Bogosian *never* stores a fingerprint along with attempted transaction information because Bogosian does not allow *any* transaction to be attempted within a system once the fingerprint is taken. In this regard, Bogosian actually teaches away from the recited audit log storage by suggesting that fingerprint information should only be taken prior to confiscating a user's means to effect *any* transaction.

A simple, non-limiting example illustrates the shortcomings of Bogosian and its stark differences with the recited features of claim 1. A user practicing an embodiment of the invention of claim 1 may use a computer mouse to attempt to buy an item for $5 from the internet by clicking on a button labeled "purchase item - $5." The invention of claim 1 may check the user's fingerprint against an authorization profile to determine if this particular user is allowed to make such a purchase (such a feature, as described above, is totally absent from Bogosian). If so, the transaction can proceed and an audit log entry may be created. For the sake of example, assume the transaction is allowed, and the user makes her purchase; an audit log entry may show that this particular user made a $5 purchase.

Now, the same user clicks on a button labeled "purchase item - $1000." The invention of claim 1 may again check the fingerprint against the authorization profile, but this time it may determine that the user is not allowed to make such an expensive purchase. Access is correspondingly denied to perform this one specific transaction within the system, and the invention stores the user's fingerprint along with her attempted transaction information (*i.e.*, the

audit log makes an entry saying that this particular person with this particular fingerprint attempted to buy something for $1000 but was denied).

Such features are nowhere disclosed or even suggested by the cited art. Bogosian simply discloses that if a user's fingerprint does not match an owner's fingerprint, a credit card should be confiscated prior to any use, and the user's fingerprint should be stored. This functionality, however, does not amount to a teaching or suggestion of storing user identification information and attempted transaction information in response to a denial of access to perform a specific transaction within an electronic system.

3. Automatic Teller Machines do not disclose or suggest the claimed authorization profile storage

In the first office action for this appealed application, which was incorporated into the final office action being appealed, the Examiner appeared to argue (without support) that information printed on a receipt of an Automatic Teller Machine (such as time information and deposit information) is equivalent to the recited authorization profile storage. Such an assertion is simply wrong. Moreover, this exact rejection was previously lodged (and then withdrawn) by the Examiner following extensive arguments presented by the Applicant.

Repeating arguments that were previously successful in removing this rejection, Applicant asserts that the Examiner has failed to establish a *prima facie* case of obviousness with respect to an Automatic Teller Machines (ATM) because (a) an ATM machine does not teach or suggest the features of independent claims 1 and (b) even if an ATM were combined with the cited art, the combination would not result in the claimed invention.

a) An ATM does not teach or suggest the claimed authorization profile storage or audit log storage

The fact that an ATM may produce a date and/or time stamp receipt does not amount to a teaching or suggestion of the recited authorization profile storage, which in one embodiment may specify specific user(s) who can perform certain specific transactions upon specific machines at, for instance, specific times and dates. [*See* Specification pages 14-15]. At most, the date and time stamp of an ATM machine (and the printing of withdrawal, deposit, and/or balance information as mentioned by the Examiner) arguably suggests that (a) a "stamp" may be created after certain transactions and (b) the "stamp" may be printed upon a receipt within the ATM machine. However, such a feature does not amount to a *prima facie* showing of obviousness, which requires disclosures in the prior art to teach or suggest all the claim limitations to a person of ordinary skill in the art. *See* M.P.E.P. § 2142, *see also*, *In re Rijckaert*, 9 F.3d 1531 (Fed. Cir. 1993).

Likewise, an ATM machine does not teach or suggest the presently recited audit log storage. Particularly, the fact that an ATM may keep a bank card if a user repeatedly enters an incorrect personal identification number (PIN) does not amount to even a suggestion of the claimed audit log storage. In particular, the Examiner has not identified any ATM (nor is Applicant aware of any ATM) having the ability to store:

(a) user identification information from a biometric sensor in response to a denial of access to an electronic system; and

(b) user identification information from the biometric sensor and attempted transaction information in response to a denial of access to perform a specific transaction within the electronic system.

At most, the bank card retention feature of ATMs arguably suggests a mechanism for counting incorrect personal identification number entries; however, such a feature does not even

approach a *prima facie* showing of obviousness, which, again, requires a teaching or suggestion of each and every claim limitation.

b) Even a combination of the cited art with ATM technology does not render the invention obvious

Even if a combination were made between, for instance, Matchett and an ATM machine, one would not arrive at the claimed invention. Specifically, if one were to combine the system of Matchett with the ATM features cited, *via* incorporation, in the final office action, the resulting system would not include the recited verification features of claim 1. Rather, it appears that the combination would result in a biometric-oriented system (Matchett) that may include the ability to produce date/time stamps and to restrict access in response to repeated, failed access attempts (an ATM machine). Such a system, however, is in stark contrast to the recited invention of claim 1, which includes a user storage, an authorization profile storage, and an audit log storage.

C. Matchett in view of Bogosian and Applicant's disclosure does not render claims 7-9, 20, or 21 unpatentable

Claims 7-9, 20, and 21 stand or fall with claim 1. Thus, those claims, rejected by the Examiner as being unpatentable over Matchett in view of Bogosian and further in view of "Applicant's prior art," should be allowed for at least the reasons stated above regarding claim 1.

D. Matchett in view of Bogosian and Bidiville does not render claims 15-19 unpatentable

Claims 15-19 stand or fall with claim 1. Thus, those claims, rejected by the Examiner as being unpatentable over Matchett in view of Bogosian and further in view of Bidiville, should be allowed for at least the reasons stated above regarding claim 1.

E. Matchett in view of Bogosian and O'Connor does not render claims 22-24 unpatentable

Claims 22-24 stand or fall with claim 1. Thus, those claims, rejected by the Examiner as being unpatentable over Matchett in view of Bogosian and further in view of O'Connor., should be allowed for at least the reasons stated above regarding claim 1.

F. The cited art, taken alone or in any combination, does not render claims 61 and 67-81 unpatentable

As stated by the Examiner, "Claims 61, 67-70, 71-78 and 79-81 are rejected as claims 1-24 and 49-60, because claims 61, 67-70, 71-78 and 79-81 are claiming similar subject matter as claims 1-24 and 49-60." Because each of independent claims 61, 67, 71, and 79 involve the authorization profile storage and audit log storage, Applicant's argument are similar to those arguments advanced above and will only be summarized here.

1. None of the cited art, taken alone or in combination, renders claim 61 unpatentable

Independent claim 61 is similar to claim 1 except that it is configured to read biometric information of a user's toe instead of a user's finger. [*See* claims 1 and 61]. Claim 61 recites the identical verification system features cited in claim 1 — including the authorization profile storage and audit log storage. Because none of the cited art, individually or in combination, disclose or suggest the authorization profile storage or the audit log storage (or the combination of the two), claim 61 is allowable.

2. None of the cited art, taken alone or in combination, renders claim 67 unpatentable

Independent claim 67 recites a computer verification system for use with a biometric sensor that includes the authorization profile and audit log storage of claims 1 and 61. Accordingly, claim 67 is patentable because none of the cited art teach or suggest such features (individually or in combination). Dependent claims 68-70 stand or fall with claim 67.

3. None of the cited art, taken alone or in combination, renders claim 71 unpatentable

Independent claim 71 recites a method for verifying a user of an electronic system coupled to a biometric sensor and includes functionality of the authorization profile and audit log storage of claims 1, 61, and 67. In particular, claim 71 recites, in part:

> comparing the selection with authorization information stored in an authorization profile;
>
> determining if the user is authorized to perform the selection; and
>
> storing identification information and attempted transaction information of the user in the audit log storage if the user is denied access to perform the selection within the electronic system.

The method of claim 71 is patentable because none of the cited art teach or suggest the features cited above. Specifically, the art does not even address the claimed authorization profile or audit log functionality discussed herein. Accordingly, claim 71 is patentable. Dependent claims 72-78 stand or fall with claim 71.

4. None of the cited art, taken alone or in combination, renders claim 79 unpatentable

Independent claim 79 recites a verification system for operably communicating with an electronic system and includes the authorization profile storage and audit log storage of claims 1, 61, 67, and 71. In particular, claim 79 recites, in part:

the verification system comprising a user storage, an authorization profile storage, and an audit log storage, the audit log storage being configured to store information in response to a successful transaction attempt and grant of access with said electronic system and to a denial of access to said electronic system and denials of access to perform specific actions within said electronic system.

The system of claim 79 is patentable because none of the cited art teach or suggest the features cited above. Specifically, the art does not even address the claimed authorization profile storage or audit log storage discussed herein. Accordingly, claim 79 is patentable. Dependent claims 80 and 81 stand or fall with claim 79.

G. Matchett in view of Bogosian and Axelrod does not render claims 57 and 58 unpatentable

Claims 57 and 58 stand or fall with claim 1. Thus, those claims, rejected by the Examiner as being unpatentable over Matchett in view of Bogosian and further in view of Axelrod, should be allowed for at least the reasons stated above regarding claim 1.

IX. CONCLUSION

This appeal brief is believed to completely address all unresolved issues relating to this application. In light of the arguments made herein, the Board is respectfully requested to reverse the current rejections directed to claims 1, 2, 7-24, 49-58, 60-61, and 67-81 and to allow those claims to pass to issue.

Please date stamp and return the enclosed postcard to evidence receipt of this document.

Respectfully submitted,

Michael C. Barrett

Michael C. Barrett
Reg. No. 44,523
Attorney for Applicants

FULBRIGHT & JAWORSKI L.L.P.
600 Congress Avenue, Suite 2400
Austin, Texas 78701
(512) 474-5201 (voice)
(512) 536-4598 (fax)
mbarrett@fulbright.com
www.fulbright.com

Date: June 11, 2002